AMENDMENTS

In the Claims:

1. (Previously Presented) A computer system comprising:

memory; and

a security application configured to lock down resources of said computer system by modifying a machine state of said computer system in response to a request for activating an original state of a security profile for a user, said security application configured to store data indicative of said machine state in said memory, said security application configured to modify said machine state in response to a request for activating a new state of said security profile for said user, said security application configured to retrieve said data in response to a request for recovering said original state of said security profile and to modify said machine state based on said retrieved data thereby activating said original state of said security profile for said user.

2. (Previously Presented) The system of claim 1, wherein said security application includes default data defining default levels of security, wherein said security application enables a user to select one of said default levels of security, and wherein said security application is configured to modify said machine state in response to said request for activating said original state of said security profile based on said selected default level of security.

3. (Previously Presented) The system of claim 2, wherein said security application defines a plurality of rules for locking down said computer system, wherein said security application configured to enable ones of said rules based on which of said default levels is selected by said user, and wherein said security application is further configured to cause said computer system to enforce each enabled rule within said plurality of rules by modifying said machine state in response to said request for activating said original state of said security profile.

4. (Original) The system of claim 3, wherein said security application enables said user to change which of said rules are enabled.

5. (Previously Presented) A computer system, comprising:

memory; and

a security application defining a plurality of rules, said security application configured to enable a user to select a set of said rules to define an original state of a security profile for a user, said security application configured to lock down said computer system by causing said computer system to enforce said selected set of rules in response to an activation request, said security application further configured to store data indicative of said original state of said security profile, said security application configured to change said security profile for said user from said original state to a new state by changing which of said plurality of rules are enforced by said computer system based on inputs to said computer system, said security application configured to retrieve said data in response to a user request and to automatically identify said set of rules based on said retrieved data, said security application further configured to return said security profile for said user to said original state thereby causing said computer system to enforce said identified rules in response to said user request.

6. (Original) The system of claim 5, wherein said security application is further configured to define multiple sets of default data, each of said sets of default data identifying different ones of said rules as being enabled for enforcement, said security application configured to enable said user to select one of said sets of default data and to determine which of said rules are selected for inclusion into said selected set of rules based on which of said rules are indicated as enabled.

7. (Original) The system of claim 6, wherein said security application enables said user to change which of said rules are indicated as being enabled.

8. (Previously Presented) A computer system comprising:

means for storing data; and

means for locking down resources of said computer system by modifying a machine state of said computer system in response to a request for activating an original state of a security profile for a user, said locking down means including a means for storing security profile data indicative of said machine state in said memory in response to said request for activating said original state of said security profile, said locking down means including a means for modifying said machine state in response to a request for activating a new state of said security profile for said user, said locking down means including a means for retrieving said security profile data in response to a request for recovering said original state of said security profile and for modifying said machine state based on said retrieved data thereby activating said original state of said security profile for said user.

9. (Previously Presented) A method for locking down resources of a computer system, comprising:

receiving a request for activating a an original state of a security profile for a user;

modifying a machine state of said computer system in response to said request for activating said original state of said security profile;

storing data indicative of said machine state;

modifying said machine state in response to a request for activating a new state of said security profile for said user;

retrieving said data in response to a request for recovering said original state of said security profile; and

modifying said machine state based on said retrieved data in response to said request for recovering said first security profile.

10. (Previously Presented) The method of claim 9, further comprising:

defining default levels of security; and

selecting one of said default levels of security,

wherein said modifying that is performed in response to said request for activating said original state of said security profile is based on said selecting.

11. (Previously Presented) The method of claim 10, further comprising:

defining a plurality of rules for locking down said computer system;

associating each of said default levels of security with different ones of said rules;

enabling ones of said rules based on which of said rules are associated, via said associating step, with said default level selected in said selecting; and

enforcing each of said rules enabled via said enabling based on said machine state as modified via said modifying that is performed in response to said request for activating said original state of said security profile.

12. (Previously Presented) The method of claim 11, further comprising:

enabling a user to change which of said rules are enabled.

13. (Previously Presented) A method for locking down resources of a computer system, comprising:

defining a plurality of rules for locking down said computer system;

receiving an input from a user of said computer system;

selecting a set of said rules based on said input;

causing said computer system to enforce said selected set of rules in response to an activation request;

storing data identifying said selected set of rules in response to said activation request;

changing which of said plurality of rules are enforced by said computer system;

detecting an operational problem caused by said changing;

providing a request to change a security state of said computer system in response to said detecting;

retrieving said data in response to said request to change said security state;

automatically identifying said selected set of rules based on said retrieved data; and

causing said computer system to enforce said selected set of rules in response to said request to change said security state.

14. (Previously Presented) The method of claim 13, further comprising:

defining multiple sets of default data, each of said sets of default data identifying different ones of said rules as being enabled; and

selecting one of said sets of default data,

wherein said selecting a set of said rules is further based on which of said sets of default data is selected via said selecting one of said sets of default data.

15. (Previously Presented) The system of claim 1, wherein said original state grants access to a particular resource of said computer system based on a user identifier, and wherein said new state denies access to said particular resource based on said user identifier.

16. (Previously Presented) The system of claim 1, further comprising an operating system configured to read said machine state modified by said security application and to control access to at least one resource of said computer system based on said machine state.

17. (Previously Presented) The computer system of claim 16, wherein said machine state read by said operating system comprises a flag indicative of whether access to said at least one resource is restricted.

18. (Previously Presented) The computer system of claim 17, wherein said operating system is configured to analyze, in response to said flag, data indicating which users are authorized to access said at least one resource.

19. (Previously Presented) The system of claim 1, wherein said security application, by activating said original state in response to said request for recovering said original state, enables said user to undo an error in defining said new state of said security profile for said user.

20. (Previously Presented) The method of claim 9, further comprising:

detecting an operational problem caused by activation of said new state of said security profile; and

providing said request for recovering said original state of said security profile in response to said detecting.

21. (Previously Presented) The method of claim 9, wherein said storing is in response to said request for activating said original state of said security profile.

22. (Previously Presented) A computer system, comprising:

memory; and

a security application configured to define a security profile for controlling access to at least one resource of said computer system, said security application configured to activate an original state of said security profile and to store data indicative of said original state in said memory, said security application further configured to activate a new state of said security profile in response to a user request, said security application further configured to enable a user to undo an error in defining said new state by allowing said user to initiate activation of said original state based on said data.